

08/29/00



09/16/00 U.S. PTO

08-30-00

09/16/00 U.S. PTO



08/29/00

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

**PATENT APPLICATION
TRANSMITTAL LETTER**

ATTORNEY DOCKET NO.:
10746/20

Address to:
Commissioner of Patents and Trademarks
Washington D.C. 20231
Box Patent Application

Transmitted herewith for filing is the patent application of

Inventor(s): **Hideki AKASHIKA, Shinichi HIRATA, Nagaaki OHYAMA and Akio KOKUBU**

For : **DATA STORING SYSTEM, ISSUING APPARATUS, DATA PROVIDING APPARATUS AND COMPUTER READABLE MEDIUM STORING DATA STORING PROGRAM**

Enclosed are:

1. **37** sheets of specification, **35** sheets of claims, and 1 sheet of abstract.
2. **16** sheet(s) of drawings.
3. Declaration and Power of Attorney.
4. Assignment to **Nippon Telegraph and Telephone Corporation**.
5. An Information Disclosure Statement.

The filing fee has been calculated as shown below:

	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)
BASIC FEE				690.00
TOTAL CLAIMS	44 - 20 =	24	18.00	432.00
INDEPENDENT CLAIMS	10 - 3 =	7	78.00	546.00
MULTIPLE DEPENDENT CLAIM PRESENT			260.00	
*Number extra must be zero or larger			TOTAL	1,668.00
If applicant is a small entity under 37 C.F.R. §§ 1.9 and 1.27, then divide total fee by 2, and enter amount here.			SMALL ENTITY TOTAL	

09/16/00 U.S. PTO

6. Please charge the required application filing fee of \$1,668.00 to the deposit account of **Kenyon & Kenyon**, deposit account number **11-0600**.
7. The Commissioner is hereby authorized to charge payment of any additional fees associated with this communication and during the pendency of this application or credit any overpayment to the deposit account of **Kenyon & Kenyon**, deposit account number **11-0600**.
8. A duplicate of this sheet is enclosed.

Dated: August 29, 2000

By: Edward W. Greason

Edward W. Greason, (Reg. No. 18,918)

KENYON & KENYON
One Broadway
New York, New York 10004
(212) 425-7200 (phone)
(212) 425-5288 (facsimile)

00550323-002900

00650323 082900

SPECIFICATION

TO ALL WHOM IT MAY CONCERN:

BE IT KNOWN THAT WE, Hideki Akashika, a citizen of Japan residing at Koutou-ku, Tokyo-to, Japan, Shinichi Hirata, a citizen of Japan residing at Zushi-shi, Kanagawa-ken, Japan, Nagaaki Ohyama, a citizen of Japan residing at Kawasaki-shi, Kanagawa-ken, Japan and Akio Kokubu, a citizen of Japan residing at Minato-ku, Tokyo-to, Japan have invented certain new and useful improvements in

DATA STORING SYSTEM, ISSUING APPARATUS, DATA
PROVIDING APPARATUS AND COMPUTER READABLE
MEDIUM STORING DATA STORING PROGRAM

of which the following is a specification:-

EL594605483 US

TITLE OF THE INVENTION

DATA STORING SYSTEM, ISSUING APPARATUS,
DATA PROVIDING APPARATUS AND COMPUTER READABLE
MEDIUM STORING DATA STORING PROGRAM

5

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a data
storing system, an apparatus and a computer readable
10 medium storing a data storing program. More
particularly, the present invention relates to a
data storing system, an apparatus and a computer
readable medium storing a data storing program for
storing data such as a program into an IC card and
15 the like by using a telecommunication system and the
like.

2. Description of the Related Art

Recently, a data storing system which uses
an apparatus having a high level of security such as
20 an IC card is becoming popular. An issuer (an IC
card issuer) stores an important data such as a
program in the apparatus when the issuer issues the
apparatus.

MULTOS is an example of a conventional
25 system wherein a system, called MULTOS-CA, which
guarantees data has authority to store a program to
a user apparatus (for example, an IC card) for
retaining security, and the issuer (IC card issuer)
in MULTOS stores the program in the user apparatus.
30 Therefore, there are problems that a data provider (a
service provider) which provides a program can not
let a user store the program which the data provider
provides, and that the data provider can not manage
information on storing a program.

35 In addition, there is no means for knowing
that a valid issuer and a valid data provider
acknowledges user's operation in which the user adds,

00650322.082900

changes, deletes data. Thus, there is a problem that data can not be stored in a user apparatus safely via network and the like.

Therefore, a data provider can store data
5 only in a card which is issued by a specific IC card provider. That is, the data provider can not store data in a card which is issued by an IC card issuer which has no relation to the data provider. Therefore, it is needed that a data provider can
10 store data safely into a card which is issued by any IC card issuer by performing certification with reliability.

SUMMARY OF THE INVENTION

15 It is an object of the present invention that the card issuer and the service provider equally can store and delete data in a card safely by mutual agreement between the user, the card issuer and the service provider.

20 Another object of the present invention is that each of the card issuer and the service provider can obtain information on data which is stored in an IC card.

Another object of the present invention is
25 to register and manage the card issuer, the service provider and the user apparatus such that mutual certification can be performed. That is, the object is that the service provider can store data safely to a user apparatus and an issuer which are not any
30 specific apparatus or issuer.

According to a first aspect of the present invention, the above object of the present invention is achieved by a data storing system comprising:

a user apparatus which stores data;
35 an issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate;

09650323.062900

a data providing apparatus which is held
by a data provider that provides data;

an issuer registration apparatus which is
held by an issuer registrar that registers and
5 manages the issuer; and

a data registration apparatus which is
held by a data registrar that registers and manages
the data provider;

wherein the user apparatus comprises:

10 a registration information generation part
which generates registration information on a key
including a user public key or a part of a secret
key, sends the registration information to the
issuing apparatus with user information; and

15 a registration verification part which
verifies a registration certificate, received from
the issuing apparatus, which is signature
information or a hash value of the issuer for the
registration information and the user information,
20 stores the registration certificate to a storage
device when the registration certificate is
verified;

wherein the issuing apparatus comprises a
registration generation part which generates the
25 registration certificate and sends the registration
certificate to the user apparatus.

In the data storing system, the user
apparatus may further comprises:

a part which sends the registration
30 certificate and storing data information to the
issuing apparatus;

a part which verifies a storing
authorization when the storing authorization is
received from the issuing apparatus;

35 a part which verifies that the storing
data information corresponds to storing data which
is acquired; and

00550323.002900

a part which stores the storing data into the storage device when it is verified that the storing data information corresponds to the storing data;

5 the issuing apparatus further comprising:
 a part which verifies the registration certificate and the storing data information which are received from the user apparatus;

 a part which provides certificate
10 information to the registration certificate and the storing data information for generating a storing authorization request when the registration certificate and the storing data information are verified; and

15 a part which sends the registration certificate, the storing data information and the storing authorization request to the data providing apparatus;

 a part which verifies a storing
20 authorization which is received from the data providing apparatus; and

 a part which sends the storing authorization to the user apparatus when the storing authorization is verified;

25 the data providing apparatus further comprising:

 a part which verifies the storing authorization request;

 a part which provides certificate
30 information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a storing authorization, and sends the storing authorization to the issuing apparatus.

35 According to a second aspect of the present invention, the above object of the present invention is achieved by an issuing apparatus in a

006280-22605560

09550323-002000

data storing system which comprises: a user apparatus which stores data; the issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate; a data providing apparatus which is held by a data provider that provides data; an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider, the issuing apparatus comprising: a part which receives user information and registration information on a key including a user public key or a part of a secret key from the user apparatus; and a registration generation part which generates registration certificate from the registration information and the user information, and sends the registration certificate to the user apparatus.

According to a third aspect of the present invention, the above object of the present invention is achieved by a data providing apparatus in data storing system which comprises: a user apparatus which stores data; an issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate; the data providing apparatus which is held by a data provider that provides data; an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider, wherein the user apparatus comprises: a registration information generation part which generates registration information on a key including a user public key or a part of a secret

key, sends the registration information to the issuing apparatus with user information; and

5 a registration verification part which verifies a registration certificate, received from the issuing apparatus, which is signature information or a hash value of the issuer for the registration information and the user information, stores the registration certificate to a storage device when the registration certificate is
10 verified;

wherein the issuing apparatus comprises a registration generation part which generates the registration certificate and sends the registration certificate to the user apparatus,

15 the data providing apparatus comprising:

a part which receives the certificate registration, storing data information and a storing authorization request from the issuing apparatus;

a part which verifies the storing
20 authorization request;

a part which provides certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a
25 storing authorization, and sends the storing authorization to the issuing apparatus.

According to a fourth aspect of the present invention, the above object of the present invention is achieved by a computer readable medium
30 storing program code for causing a data storing system to store data, the data storing system comprising: a user apparatus which stores data; an issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages
35 a registration certificate; a data providing apparatus which is held by a data provider that provides data; an issuer registration apparatus

00650323-002900

which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider; the

5 computer readable medium comprising:

registration information generation program code means, provided for the user apparatus, which generates registration information on a key including a user public key or a part of a secret

10 key, sends the registration information to the issuing apparatus with user information; and

registration verification program code means, provided for the user apparatus, which verifies a registration certificate, received from

15 the issuing apparatus, which is signature information or a hash value of the issuer for the registration information and the user information, stores the registration certificate to a storage device when the registration certificate is

20 verified;

registration generation program code means, provided for the issuing apparatus, which generates the registration certificate and sends the registration certificate to the user apparatus.

25 The computer readable medium may further comprises:

program code means, provided for the user apparatus, which sends the registration certificate and storing data information to the issuing

30 apparatus;

program code means, provided for the user apparatus, which verifies a storing authorization when the storing authorization is received from the issuing apparatus;

35 program code means, provided for the user apparatus, which verifies that the storing data information corresponds to storing data which is

05650323.00000

acquired; and

program code means, provided for the user
apparatus, which stores the storing data into the
storage device when it is verified that the storing
5 data information corresponds to the storing data;

program code means, provided for the
issuing apparatus, which verifies the registration
certificate and the storing data information which
are received from the user apparatus;

10 program code means, provided for the
issuing apparatus, which provides certificate
information to the registration certificate and the
storing data information for generating a storing
authorization request when the registration
15 certificate and the storing data information are
verified; and

program code means, provided for the
issuing apparatus, which sends the registration
certificate, the storing data information and the
20 storing authorization request to the data providing
apparatus;

program code means, provided for the
issuing apparatus, which verifies a storing
authorization which is received from the data
25 providing apparatus; and

program code means, provided for the
issuing apparatus, which sends the storing
authorization to the user apparatus when the storing
authorization is verified;

30 program code means, provided for the data
providing apparatus, which verifies the storing
authorization request;

program code means, provided for the data
providing apparatus, which provides certificate
35 information to the storing authorization request and
the storing data information when the storing
authorization request is verified for generating a

00000000-00000000

storing authorization, and sends the storing authorization to the issuing apparatus.

According to a fifth aspect of the present invention, the above object of the present invention is achieved by a computer readable medium storing program code for causing an issuing apparatus in a data storing system to perform processes, the data storing system comprising: a user apparatus which stores data; the issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate; a data providing apparatus which is held by a data provider that provides data; an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider, the computer readable medium comprising: program code means which receives user information and registration information on a key including a user public key or a part of a secret key from the user apparatus; and

registration generation program code means which generates registration certificate from the registration information and the user information, and sends the registration certificate to the user apparatus.

According to a sixth aspect of the present invention, the above object of the present invention is achieved by a computer readable medium storing program code for causing a data providing apparatus in a data storing system to perform processes, the data storing system comprising: a user apparatus which stores data; an issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate; the data providing apparatus which is held by a data

09650323-082900

invention, the user apparatus generates the registration information, sends it to the issuing apparatus with user information. The issuing apparatus stores the received registration
5 information and the user information, provides certificate information to the registration information, generates registration certificate, sends it to the user apparatus. The user apparatus verifies the received registration certificate,
10 stores it in a storage device if it is verified, such that data in an IC card can be stored and deleted safely.

According to the above-mentioned invention, by using the registration certificate which is
15 issued by the registration issuer, the party which receives the registration is insured. In addition, both of the card issuer and the service provider can perform processes such as data storing and data deleting safely.

20 In addition, the issuing apparatus, the data providing apparatus and the user apparatus verifies the registration certificate, the storing authorization request and the storing authorization such that tampering by a third party is prevented.

25 Further, each of the card issuer and the service provider can obtain information on data which is stored an IC card.

BRIEF DESCRIPTION OF THE DRAWINGS

30 Other objects, features and advantages of the present invention will become more apparent from the following detailed description when read in conjunction with the accompanying drawings, in which:

35 Fig.1 is a figure showing the principle of the present invention;

Fig.2 is a block diagram of a data storing

00550323-002900

system of the present invention;

Fig.3 is a diagram for explaining a general outline of the operation of the data storing system:

5 Fig.4 shows a system configuration for
user registration according to a first embodiment of
the present invention;

Fig.5 is a diagram for explaining a
general outline of the operation of the data storing
10 system when data is stored via an issuer according
to a second embodiment;

Fig.6 is a block diagram of the data storing system when data is stored via the issuer according to the second embodiment;

15 Fig.7 is a diagram for explaining a
general outline of the operation of the data storing
system when data is stored via an data provider
according to a third embodiment;

Fig.8 is a block diagram of the data
20 storing system when data is stored via the data
provider according to the third embodiment;

Fig.9 is a diagram for explaining a
general outline of the operation of the data storing
system when data is stored only by the data provider
25 according to a fourth embodiment;

Fig.10 is a block diagram of the data storing system when data is stored only by the data provider according to the fourth embodiment;

Fig.11 is a diagram for explaining a
30 general outline of the operation of the data storing
system when a user apparatus is registered according
to a fifth embodiment;

Fig.12 is a block diagram of the data storing system when a user apparatus is registered according to the fifth embodiment;

Fig.13 is a diagram for explaining a general outline of the operation of the data storing

system when data is stored according to a sixth embodiment;

Fig.14 is a block diagram of the data storing system when data is stored according to the sixth embodiment;

Fig.15 is a block diagram of the data storing system when data is stored according to a seventh embodiment;

Fig.16 is a block diagram of a computer system which can be used as an issuing apparatus, a data providing apparatus and the like.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Fig.1 and Fig.2 are figures of a data storing system for explaining the principle of the present invention. The data storing system includes a user apparatus 300 which stores data; an issuing apparatus 100 which is held by an issuer that provides the user apparatus 300, issues and manages a registration certificate; a data providing apparatus 200 which is held by a data provider that provides data; an issuer registration apparatus 400 which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus 500 which is held by a data registrar that registers and manages the data provider.

In the above-mentioned configuration, the user apparatus includes a registration information generation part 320 which generates registration information on a key including a user public key or a part of a secret key, sends the registration information to the issuing apparatus 100 with user information; and a registration verification part 330 which verifies a registration certificate which is received from the issuing apparatus and which is signature information or a hash value of the issuer for the registration information and the user

09550323-002900

The issuing apparatus 100 includes a
5 registration generation part 120 which generates the
registration certificate and sends the registration
certificate to the user apparatus.

As mentioned above, as shown in Fig.2, the data storing system of the present invention includes an issuing apparatus 100, a data providing apparatus 200, a user apparatus 300, an issuer registration apparatus 400 and a data registration apparatus 500. The issuing apparatus 100 is owned by an issuer which provides the user apparatus, issues and manages a registration certificate. The data providing apparatus 200 is owned by a data provider which provides data. The user apparatus 300 stores the registration certificate and the data. The issuer registration apparatus 400 is owned by an issuer registrar which insures validity of the registration certificate. The data registration apparatus 500 is owned by a data registrar which insures validity of data.

The issuing apparatus 100, the data providing apparatus 200, the issuer registration apparatus 400 and the data registration apparatus 500 generate and retain key information (such as a public key, a private key, a shared key, a part of a secret key and the like) for generating and

5 "CONTEMPORARY ENCRYPTION THEORY", Ikeno, Koyama,
IEICE.

In the following, a general outline of the operation of an embodiment of the present invention will be described with reference to Fig.3. Each of the issuer registration apparatus and the data registration apparatus issues a registration certificate for the issuing apparatus and the data providing apparatus respectively by using a signature or the like. According to the registration certificate, each of the issuing apparatus and the data providing apparatus can be proved to be valid.

The issuing apparatus issues a registration certificate to the user apparatus. An application can be downloaded into the user apparatus via the issuing apparatus or via the data providing apparatus. An authorization for storing data is exchanged between the issuing apparatus and the data providing apparatus.

25 In the following, embodiments of the
present invention will be described with reference
to figures.

(first embodiment)

A first embodiment will be described with reference to Fig.4. In this embodiment, the process of user registration between the user apparatus 300 and the issuing apparatus 100 will be described.

Fig.4 shows a system configuration for user registration of the first embodiment. This system includes the issuing apparatus 100 and the user apparatus 300. The issuing apparatus 100 includes a database 110 and a certificate generation

part 120. The certificate generation part 120 generates a digital signature (or encrypted data, or secure hash) for proving that the issuer generates a registration certificate from input data. As the
5 input data, information (RI) on a key such as a user public key (public key, symmetric key in symmetric key cryptography or the like) and user information (UID) which includes a user identifier are input from the user apparatus 300. The certificate
10 generation part 120 generates the digital signature (or encrypted data, or secure hash) of the issuer for the registration information (RI) and the user information (UID) which are input from the user apparatus 300. The registration generation part 120
15 outputs these data to the user apparatus 300 as a registration certificate (RC). In the above configuration, the issuing apparatus 100 may generate the registration information (RI) and the user information (UI) instead of receiving them from
20 the user apparatus 300. In such a case, the issuing apparatus 100 includes a registration information generation part.

The user apparatus 300 includes a memory
25 310, a registration information generation part 320 and a certificate verification part 330.

The registration information generation part 320 generates the registration information (RI) and the user information (UID), and stores these information into the memory 310.

30 The certificate verification part 330 verifies validity of the registration certificate (RC) input from the issuing apparatus 100. The certificate verification part 330 verifies the digital signature (or encrypted data, or secure
35 hash) of the registration certificate (RC). When the registration certificate is valid, the certificate verification part 330 stores the

0050322-00200

registration certificate (RC) into the memory 310.

The operation of user registration is as follows.

(Step 11) The registration information
5 generation part 320 in the user apparatus 300
generates the registration information for the
issuing apparatus 100, stores the registration
information (RI) into the memory 310, and sends the
registration information (RI) to the issuing
10 apparatus 100. When the issuing apparatus issues
the registration information, this step 11 is not
performed.

(Step 12) The certificate generation part
120 in the issuing apparatus 100 generates a
15 registration certificate (RC) from the registration
information (RI), stores it in the database 110, and
sends it to the user apparatus 300.

(Step 13) The certificate verification
part 330 in the user apparatus 300 verifies the
20 registration certificate (RC), and stores the
registration certificate (RC) in the memory 310 if
it is verified.

(Second embodiment)

In this embodiment, the process of storing
25 data (downloading of application) via the issuer
will be described. First, the general outline will
be described with reference to Fig.5.

In this process, the data registration
apparatus 500 issues a data provider registration
30 certificate to a data providing apparatus 200 in
advance. (the processes (1) and (2) in Fig.5.

When the user apparatus 300 requests
application download to the issuing apparatus 100 in
step 21, the issuing apparatus 100 sends a storing
35 authorization request to the data providing
apparatus 200 in step 22. The data providing
apparatus 200 issues a storing authorization to the

00550323-08200

issuing apparatus 100 in step 23. Then, the issuing apparatus 100 downloads a requested application to the user apparatus 100 in step 24.

Next, the second embodiment will be
5 described in detail with reference to Fig.6. Fig.6 is a block diagram of the data storing system for data storing via the issuer according to the second embodiment.

This system shown in Fig.6 includes a
10 issuing apparatus 100, a data providing apparatus 200 and a user apparatus 300.

The issuing apparatus 100 includes a
certificate generation part 120, a certificate
verification part 130 and a storing data
15 verification part 140.

The certificate verification part 130
acquires a registration certificate (RC) from the
user apparatus 300 and verifies the digital
signature (or encrypted data, or secure hash) for
20 proving that the registration certificate (RC) is
generated by the issuing apparatus 100. When the
registration certificate is verified, a storing
authorization is issued, and sent to the user
apparatus 300.

The storing data verification part 140
25 acquires storing data information (SDI) which
includes storing data identifier from the user
apparatus 300. Then, the storing data verification
part 140 verifies the storing data information (SDI).
30 When the data is verified, the verification result
(storing data information (SDI)) is sent to the
certificate generation part 120 and the data
providing apparatus 200.

The certificate generation part 120
35 receives verified a registration certificate (RC)
from the certificate verification part 130 and
receives verified storing data information (SDI)

00550323 082000

5

10

15

25

30

35

(Step 24) The issuing apparatus 100 verifies the storing authorization (SA) in the certificate verification part 130. When it is 5 verified, the issuing apparatus sends the storing authorization (SA) to the user apparatus 300.

In the above-mentioned process, the user apparatus can delete the storing data (APD) which is already in the memory 310.

20 In the third embodiment, a case wherein
data is stored via the data provider. The general
outline will be described with reference to Fig.7.

When the user apparatus 300 requests application download to the data providing apparatus 200 in step 31, the data providing apparatus 200 sends a storing authorization request to the issuing apparatus 100 in step 32. The issuing apparatus 100 issues a storing authorization to the data providing apparatus 200 in step 33. Then, the data providing apparatus 200 downloads a requested application to the user apparatus 100 in step 34.

Next, the third embodiment will be described in detail with reference to Fig.8. Fig.8

is a block diagram of the data storing system for data storing via the data provider according to the third embodiment.

This system shown in Fig.8 includes a
5 issuing apparatus 100, a data providing apparatus 200 and a user apparatus 300.

The issuing apparatus 100 includes a certificate generation part 120, a certificate verification part 130 and a storing data
10 verification part 140.

When the certificate verification part 130 acquires the storing authorization request (SAR) from the data providing apparatus 200, the certificate verification part 130 verifies the
15 storing authorization request. When it is verified, the certificate verification part 130 sends the storing data information (SDI) to the storing data verification part 140 and sends the storing authorization request (SAR) to the certificate
20 generation part 120.

The storing data verification part 140 verifies the storing data information (SDI). When it is verified, the storing data information (SDI) is sent to the certificate generation part 120.

25 The certificate generation part 120 sends a digital signature (or encrypted data, or secure hash) as the storing authorization (SA) to the data providing apparatus 200. The digital signature proves that the storing authorization (SA) is generated by
30 the issuer on the basis of the storing authorization request (SAR) received from the certificate verification part 130 and the storing data information (SDI) received from the storing data verification part 140.

35 The data providing apparatus 200 includes a database 210, a certificate generation part 220, a certificate verification part 230 and a storing data

00550323.082900

verification part 240.

The certificate verification part 230 acquires the storing authorization (SA) from the issuing apparatus 100 and acquires a registration
5 certificate (RC) from the user apparatus 300, and verifies them.

The certificate generation part 220 receives the registration certificate (RC) from the certificate verification part 230 and receives the
10 storing data information (SDI) from the storing data verification part 240. Then, the certificate generation part 220 generates a storing authorization request (SAR) from them, and sends the storing authorization request (SAR) to the issuing
15 apparatus 100.

The storing data verification part 240 acquires storing data information (SDI) from the user apparatus 300. Then, the storing data
20 verification part 240 verifies the storing data information (SDI). When it is verified, the verification result (storing data information (SDI)) is sent to the certificate generation part 220.

The user apparatus 300 includes a memory 310, a certificate verification part 330 and a data
25 verification part 340.

The registration certificate (RC) is sent to the certificate verification part 230 of the data providing apparatus 200 from the memory 310, and the
30 storing data information (SDI) is sent to the storing data verification part 240 of the data providing apparatus 200.

The certificate verification part 330 acquires the storing authorization (SA) from the certificate verification part 230 in the data
35 providing apparatus 230, verifies the storing authorization (SA), and sends the verification result to the data verification part 340 when the

09650323.082900

storing authorization (SA) is verified.

The data verification part 340 acquires storing data (APD) from the database 210 in the data providing apparatus 200, and verifies the data.

- 5 When it is verified, the data verification part 340 stores the storing data (APD) into the memory 310.

In the following, the operation of the above-mentioned configuration in which data is stored via the provider will be described in detail.

- 10 (Step 31) The user apparatus 300 sends the registration certificate (RC) and the storing data information (SDI) to the data providing apparatus 200.

- (Step 32) The data providing apparatus 200
15 verifies the registration certificate (RC) in the certificate verification part 230, and verifies the storing data information (SDI) in the storing data verification part 240. When both of them are verified, the data providing apparatus 200 generates
20 the storing authorization request (SAR) based on the registration certificate (RC) and the storing data (SDI) in the certificate generation part 220, and sends the registration certificate (RC), the storing data (SDI) and the storing authorization request
25 (SAR) to the issuing apparatus 200.

- (Step 33) The issuing apparatus 100
verifies the storing authorization request (SAR) in the certificate verification part 130, and verifies
30 the storing data information (SDI) in the storing data verification part 140. When both of them are verified, the issuing apparatus 100 generates a storing authorization (SA) for the storing authorization request (SAR) and the storing data information (SDI) in the certificate generation part
35 120, and sends the storing authorization (SA) to the data providing apparatus 100.

(Step 34) The data providing apparatus 200

00550323-002900

5 Then, the user apparatus 300 verifies the
storing authorization (SA) by using the certificate
verification part 330. The user apparatus 300
verifies that the storing data information (SDI)
corresponds to storing data (APD) which is received
10 in some way by using the data verification part 340.
When it is verified, the storing data (APD) is
stored in the memory 310.

(fourth embodiment)

In this embodiment, the data registration
500 issues a data provider registration
to the data providing apparatus 200 in
(the processes (1) and (2) in Fig.9.)

Next, the fourth embodiment will be in detail with reference to Fig.10.

This system shown in Fig.10 includes a

data providing apparatus 200 and a user apparatus 300.

The data providing apparatus 200 includes a database 210, a certificate generation part 220, a certificate verification part 230 and a storing data verification part 240.

The certificate verification part 230 acquires a registration certificate (RC) from the user apparatus 300, and verifies it.

10 The certificate generation part 220
verifies both of the registration certificate (RC)
the storing data information (SDI). When they are
verified, the certificate generation part 220
generates a storing authorization request (SAR) from
15 them, and sends the storing authorization request
(SAR) to the user apparatus 300.

The user apparatus 300 includes a memory 310, a certificate verification part 330 and a data verification part 340.

20 The certificate verification part 330
acquires the storing authorization (SA) received
from the data providing apparatus 200, and verifies
the storing authorization (SA).

The data verification part 340 acquires
25 storing data (APD) from the data providing apparatus
200, and verifies the data. When it is verified,
the data verification part 340 stores the storing
data (APD) into the memory 310.

In the following, the operation of the
30 above-mentioned configuration in which data is
stored only by the data provider will be described
in detail.

(Step 41) The user apparatus 300 sends the registration certificate (RC) and the storing data information (SDI) to the data providing apparatus 200.

(Step 42) The data providing apparatus 200

and stores the registration certificate in a card which is provided to a user.

Next, the fifth embodiment will be described in detail with reference to Fig.12.

- 5 Fig.12 shows a block diagram of the data storing system at the time of user registration.

This system includes the issuing apparatus 100, the user apparatus 300 and the issuer registration apparatus 400.

- 10 The issuer registration apparatus 400 includes a database 410 and a certificate generation part 420.

- The certificate generation part 420 acquires information (PKI) used for providing
15 certificate information from the issuing apparatus 100, generates an issuer registration certificate (IRC), stores it into the database 410, and sends it to the issuing apparatus 100.

- The issuing apparatus 100 includes a
20 database 110, a certificate generation part 120, a certificate verification part 130 and a key information generation part 150.

- The certificate generation part 120 generates a registration certificate (RC) from
25 registration information (RI) which is received from the user apparatus 300, stores the registration certificate (RC) into the database 110, and sends it to the user apparatus 300.

- The certificate verification part 130
30 acquires the issuer registration certificate (IRC) from the issuer registration apparatus 400, and verifies the issuer registration certificate (IRC). When the issuer registration certificate (IRC) is verified, it is stored into the database 110.

- 35 The key information generation part 150 generates information (PKI) which is used for providing certificate information by the issuer.

00000000-00000000

The registration information generation
5 part 320 generates registration information of
information (RI) (a public key, a symmetric key in
symmetric key cryptography, and the like) on a key
such as a user public key or a part of a secret key
and stores it in the memory 310.

In the above configuration, the issuing apparatus 100 may generate the registration information (RI) instead of receiving the registration information (RI) from the issuing apparatus 100. In such a case, the issuing apparatus includes a registration information generation part.

(1) The issuing apparatus 100 generates information (key information) used for providing certificate information (used in the certificate generation part 120) by using the key information generation part 150, and sends the information (PKI) (key information, or a part of the key information) to the issuer registration apparatus 400.

(2) The issuer registration apparatus 400 generates the issuer registration certificate (IRC) 35 by using the information (PKI) in the certificate generation part 420. Then, the issuer registration apparatus 400 stores the information (PKI) and the

issuer registration certificate (IRC), and sends the issuer registration certificate (IRC) to the issuing apparatus 100.

5 The issuing apparatus 100 verifies the issuer registration certificate (IRC) in the certificate verification part 130. When it is verified, the issuer registration certificate (IRC) is stored in the database 110.

10 (Step 51) The user apparatus 300 generates registration information (RI) in the registration information generation part 320, stores it in the memory 310 and sends the registration information (RI) to the issuing apparatus 100. As mentioned above, the registration information (RI) can be
15 generated by the issuing apparatus.

(Step 52) The issuing apparatus 100 generates a registration certificate (RC) by using the received registration information (RI) in the certificate generation part 120, stores the
20 registration certificate in to the memory 110, and sends the registration certificate (RC) and the issuer registration certificate (IRC) to the user apparatus 300.

In addition, the user apparatus 300
25 verifies the registration certificate (RC) and the issuer registration certificate (IRC) by the certificate verification part 330. When both of them are verified, the registration certificate (RC) and the issuer registration certificate (IRC) is
30 stored in the memory 110.

(sixth embodiment)

In the following, the general outline of the sixth embodiment will be described with reference to Fig.13. In this embodiment, a
35 registration is issued to the data providing apparatus and a certificate is provided to application data.

00000323.082000

database 210. Then, the certificate generation part 220 generates storing data with a certificate (SDCI) which is the storing data (APD) and a digital signature to the storing data (APD) and the storing data information (SDI) which indicates data providing authorization. Then, the certificate generation part 220 sends the storing data (SDCI) with a certificate to the user apparatus 300.

The certificate verification part 230 acquires the data provider registration certificate (DPR) from the data registration apparatus 500 and verifies it.

The certificate verification part 330 acquires the data provider registration certificate (DPR) and the storing data with a certificate (SDCI) which is a digital signature of the data provider from the data providing apparatus 200. Then, the certificate verification part 330 verifies both of them. When they are verified, the certificate verification part 330 sends the storing data (APD) to the data verification part 340.

The data verification part 340 verifies the storing data (APD), and stored it into the memory 310 when it is verified.

The operation of the above-mentioned configuration will be described.

(1) The data registration apparatus 200 generates information (key information) used for providing certificate information (used in the certificate generation part 220) by using the key information generation part 250, and sends the information (PKD) (key information, or a part of the key information) to the data registration apparatus 500.

(2) The data registration apparatus 500 generates the data provider registration certificate (DPR) by using the information (PKD) in the

00550322.00200

used as the issuing apparatus, the data providing apparatus and the like. The program is installed in the memory 601 or the hard disk 602, and executed by the CPU 600.

5 As mentioned above, according to the present invention, the following effects can be obtained.

(1) By the registration certificate which is issued by the registration issuer, the party
10 which receives the registration is insured. In addition, both of the card issuer and the service provider can perform processes such as data storing and data deleting safely.

That is, since the public key information
15 used for a certificate is certified by the registration issued by each registrar, the validity of the authorization is insured such that both of the card issuer and the service provider perform processes safely. In addition, since the issuer
20 which is certified issues the registration certificate of a card, the validity of the card is insured.

(2) By mutual agreement between the user, the card issuer and the service provider, the card
25 issuer and the service provider equally can store and delete data in a card safely.

That is, as mentioned above, since a party issues the storing authorization to another party which performs data download, data download is not
30 performed only by one of the card issuer and the service provider without authorization by another party such that data can be stored and deleted safely.

(3) Each of the card issuer and the
35 service provider can obtain information on data which is stored in an IC card.

That is, since data download is performed

09550323-082900

after each of the user, the card issuer and the service provider reaches an agreement, each of the card issuer and the service provider can obtain information on an application and a card which
5 stores the application.

In the future, as the number of applications which are downloaded in IC cards increases, it becomes important to obtain the above-mentioned information.

10 In addition, according to the present invention, a service provider can store data to a card which is issued by any IC card issuer safely.

The present invention is not limited to the specifically disclosed embodiments, and
15 variations and modifications may be made without departing from the scope of the invention.

20

25

30

35

00650323:082900

WHAT IS CLAIMED IS:

5

1. A data storing system comprising:
 - a user apparatus which stores data;
 - an issuing apparatus which is held by an issuer that provides the user apparatus, and issues
 - 10 and manages a registration certificate;
 - a data providing apparatus which is held by a data provider that provides data;
 - an issuer registration apparatus which is held by an issuer registrar that registers and
 - 15 manages the issuer; and
 - a data registration apparatus which is held by a data registrar that registers and manages the data provider;
 - wherein the user apparatus comprises:
 - 20 registration information generation means which generates registration information on a key including a user public key or a part of a secret key, sends the registration information to the issuing apparatus with user information; and
 - 25 registration verification means which verifies a registration certificate, received from the issuing apparatus, which is signature information or a hash value of the issuer for the registration information and the user information,
 - 30 stores the registration certificate to a storage device when the registration certificate is verified;
 - wherein the issuing apparatus comprises registration generation means which generates the
 - 35 registration certificate and sends the registration certificate to the user apparatus.

09650323-082000

verified; and

means which sends the registration certificate, the storing data information and the storing authorization request to the issuing

5 apparatus;

means which verifies a storing authorization which is received from the issuing apparatus; and

10 means which sends the storing authorization to the user apparatus when the storing authorization is verified;

the issuing apparatus further comprising:

means which verifies the storing authorization request;

15 means which provides certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a storing authorization, and sends the storing
20 authorization to the data providing apparatus.

25 5. The data storing system as claimed in claim 1, the user apparatus further comprising:

means which sends the registration certificate and storing data information to the data providing apparatus;

30 means which verifies a storing authorization which is received from the data providing apparatus;

means which verifies that the storing data information corresponds to storing data which is
35 acquired;

means which stores the storing data in the storage device when it is verified that the storing

00650323-082900

issuer registration certificate to the issuing apparatus;

the user apparatus further comprising:
means which verifies the registration
5 certificate and the issuer registration certificate
which are received from the issuing apparatus; and
means which stores the registration
certificate and the issuer registration certificate
into the storage device when the registration
10 certificate and the issuer registration certificate
are verified.

15

7. The data storing system as claimed in claim 3, the data providing apparatus further comprising:

means which sends information used for
20 providing certificate information to the data
registration apparatus;
means which verifies data provider
registration certificate received from the data
registration apparatus, and stores the data provider
25 registration certificate when the data provider
registration certificate is verified;

means which generates storing data with
certificate information wherein the certificate
information is provided to the storing data, and
30 adds the data provider registration certificate to
the storing data with certificate information;

the data registration apparatus further
comprising;

means which generates the data provider
35 registration certificate wherein certificate
information is added to the information which is
received from the data providing apparatus, and

00660323-062900

sends the data provider registration certificate to the data providing apparatus;

the user apparatus further comprising;

means which verifies the storing data with

- 5 certificate information which is received from the data providing apparatus by using the data provider registration certificate, and stores the storing data into the storage device when the storing data with certificate information is verified.

10

8. The data storing system as claimed in claim 4, the data providing apparatus further comprising;

means which sends information used for providing certificate information to the data registration apparatus;

- 20 means which verifies data provider registration certificate received from the data registration apparatus, and stores the data provider registration certificate when the data provider registration certificate is verified;

- 25 means which generates storing data with certificate information wherein the certificate information is provided to the storing data, and adds the data provider registration certificate to the storing data with certificate information;

- 30 the data registration apparatus further comprising;

means which generates the data provider registration certificate wherein certificate information is added to the information which is

- 35 received from the data providing apparatus, and sends the data provider registration certificate to the data providing apparatus;

00550323.08200

the user apparatus further comprising;
means which verifies the storing data with
certificate information which is received from the
data providing apparatus by using the data provider
5 registration certificate, and stores the storing
data into the storage device when the storing data
with certificate information is verified.

10

9. The data storing system as claimed in
claim 5, the data providing apparatus further
comprising:
15 means which sends information used for
providing certificate information to the data
registration apparatus;
means which verifies data provider
registration certificate received from the data
20 registration apparatus, and stores the data provider
registration certificate when the data provider
registration certificate is verified;
means which generates storing data with
certificate information wherein the certificate
25 information is provided to the storing data, and
adds the data provider registration certificate to
the storing data with certificate information;
the data registration apparatus further
comprising;
30 means which generates the data provider
registration certificate wherein certificate
information is added to the information which is
received from the data providing apparatus, and
sends the data provider registration certificate to
35 the data providing apparatus;
the user apparatus further comprising;
means which verifies the storing data with

00000000:00000000

certificate information which is received from the data providing apparatus by using the data provider registration certificate, and stores the storing data into the storage device when the storing data with certificate information is verified.

- 10 10. The data storing system as claimed in claim 3, the data providing apparatus further comprising:
- means which sends storing data to be stored in the user apparatus and information used
- 15 for providing certificate information to the data registration apparatus;
- the data registration apparatus further comprising;
- means which generates data certificate
- 20 wherein certificate information is added to the storing information and the information which is received from the data providing apparatus, and sends the data certificate to the data providing apparatus;
- 25 the data providing apparatus further comprising:
- means which verifies the data certificate received from the data registration apparatus, and stores the data certificate when the data
- 30 certificate is verified;
- means which sends the storing data and the data certificate as storing data with certificate information to the user apparatus;
- the user apparatus further comprising;
- 35 means which receives and verifies the storing data with certificate information, and stores the storing data into the storage device when

00000000-00000000

5

15

20

30

14. An issuing apparatus in a data storing system which comprises: a user apparatus which stores data; the issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate; a data providing apparatus which is held by a data provider that provides data; an issuer registration

apparatus which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider, the issuing apparatus comprising:

means which receives user information and registration information on a key including a user public key or a part of a secret key from the user apparatus; and

registration generation means which generates registration certificate from the registration information and the user information, and sends the registration certificate to the user apparatus.

15

15. An issuing apparatus in a data storing system which comprises: a user apparatus which stores data; the issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate; a data providing apparatus which is held by a data provider that provides data; an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider, the issuing apparatus comprising:

means which generates user information and registration information on a key including a user public key or a part of a secret key; and

registration generation means which generates registration certificate from the registration information and the user information, and sends the registration certificate to the user

35

00650323 002900

apparatus.

16. The issuing apparatus as claimed in claim 14, further comprising:

```

means which receives the registration
certificate and storing data information from the
10 user apparatus;

```

means which verifies the registration certificate and the storing data information;

means which provides certificate information to the registration certificate and the
15 storing data information for generating a storing authorization request when the registration certificate and the storing data information are verified; and

means which sends the registration
20 certificate, the storing data information and the
storing authorization request to the data providing
apparatus;

means which verifies a storing
authorization which is received from the data
25 providing apparatus; and

means which sends the storing authorization to the user apparatus when the storing authorization is verified.

30

17. The issuing apparatus as claimed in claim 14, further comprising:

35 means which receives the registration
certificate, storing data information and a storing
authorization request from the data providing

apparatus;

means which verifies the storing
authorization request;

- means which provides certificate
5 information to the storing authorization request and
the storing data information when the storing
authorization request is verified for generating a
storing authorization, and sends the storing
authorization to the data providing apparatus.

10

18. The issuing apparatus as claimed in
15 claim 14, further comprising:

means which sends information used for
providing certificate information to the issuer
registration apparatus;

- means which verifies an issuer
20 registration certificate which is received from the
issuer registration apparatus;

means which stores the issuer registration
certificate when the issuer registration certificate
is verified;

- 25 means which generates the registration
certificate to the user apparatus, and sends the
registration certificate to the user apparatus with
the issuer registration certificate.

30

19. A data providing apparatus in data
storing system which comprises: a user apparatus
35 which stores data; an issuing apparatus which is
held by an issuer that provides the user apparatus,
and issues and manages a registration certificate;

the data providing apparatus which is held by a data provider that provides data; an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider, wherein the user apparatus comprises:

registration information generation means
which generates registration information on a key
10 including a user public key or a part of a secret
key, sends the registration information to the
issuing apparatus with user information; and

registration verification means which
verifies a registration certificate, received from
15 the issuing apparatus, which is signature
information or a hash value of the issuer for the
registration information and the user information,
stores the registration certificate to a storage
device when the registration certificate is
20 verified;

wherein the issuing apparatus comprises registration generation means which generates the registration certificate and sends the registration certificate to the user apparatus,

25 the data providing apparatus comprising:
 means which receives the certificate
registration, storing data information and a storing
authorization request from the issuing apparatus;
 means which verifies the storing
30 authorization request;

means which provides certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a storing authorization, and sends the storing authorization to the issuing apparatus.

0960323 259000

20. The data providing apparatus as
5 claimed in claim 19, further comprising:
means which verifies the registration
certificate and storing data information which are
received from the user apparatus;
means which provides certificate
10 information to the registration certificate and the
storing data information for generating a storing
authorization request when the registration
certificate and the storing data information are
verified; and
15 means which sends the registration
certificate, the storing data information and the
storing authorization request to the issuing
apparatus;
means which verifies a storing
20 authorization which is received from the issuing
apparatus; and
means which sends the storing
authorization to the user apparatus when the storing
authorization is verified.

21. The data providing apparatus as
30 claimed in claim 19, further comprising:
means which receives the registration
certificate and storing data information from the
user apparatus;
means which verifies the registration
35 certificate;
means which generates a storing
authorization wherein certificate information is

provided to the registration certificate and the storing data information when the registration certificate is verified, and sends the storing authorization to the user apparatus.

5

22. The data providing apparatus as
10 claimed in claim 19, further comprising:
means which sends information used for
providing certificate information to the data
registration apparatus;
means which verifies data provider
15 registration certificate received from the data
registration apparatus, and stores the data provider
registration certificate when the data provider
registration certificate is verified;
means which generates storing data with
20 certificate information wherein the certificate
information is provided to the storing data, and
adds the data provider registration certificate to
the storing data with certificate information; and
means which sends the data provider
25 registration certificate and the storing data with
certificate information to the user apparatus.

30

- ~~23.~~ A computer readable medium storing
program code for causing a data storing system to
store data, the data storing system comprising: a
user apparatus which stores data; an issuing
35 apparatus which is held by an issuer that provides
the user apparatus, and issues and manages a
registration certificate; a data providing apparatus

when the storing authorization is received from the
issuing apparatus;

program code means, provided for the user
apparatus, which verifies that the storing data
5 information corresponds to storing data which is
acquired; and

program code means, provided for the user
apparatus, which stores the storing data into the
storage device when it is verified that the storing
10 data information corresponds to the storing data;

program code means, provided for the
issuing apparatus, which verifies the registration
certificate and the storing data information which
are received from the user apparatus;

15 program code means, provided for the
issuing apparatus, which provides certificate
information to the registration certificate and the
storing data information for generating a storing
authorization request when the registration
20 certificate and the storing data information are
verified; and

program code means, provided for the
issuing apparatus, which sends the registration
certificate, the storing data information and the
25 storing authorization request to the data providing
apparatus;

program code means, provided for the
issuing apparatus, which verifies a storing
authorization which is received from the data
30 providing apparatus; and

program code means, provided for the
issuing apparatus, which sends the storing
authorization to the user apparatus when the storing
authorization is verified;

35 program code means, provided for the data
providing apparatus, which verifies the storing
authorization request;

09650323-082900

authorization request when the registration certificate and the storing data information are verified; and

5 program code means, provided for the data providing apparatus, which sends the registration certificate, the storing data information and the storing authorization request to the issuing apparatus;

10 program code means, provided for the data providing apparatus, which verifies a storing authorization which is received from the issuing apparatus; and

15 program code means, provided for the data providing apparatus, which sends the storing authorization to the user apparatus when the storing authorization is verified;

 program code means, provided for the issuing apparatus, which verifies the storing authorization request;

20 program code means, provided for the issuing apparatus, which provides certificate information to the storing authorization request and the storing data information when the storing authorization request is verified for generating a
25 storing authorization, and sends the storing authorization to the data providing apparatus.

30

27. The computer readable medium as claimed in claim 23, further comprising:

35 program code means, provided for the user apparatus, which sends the registration certificate and storing data information to the data providing apparatus;

 program code means, provided for the user

00650323.00200

program code means, provided for the user
5 apparatus, which deletes the storing data which is
in the storage device.

36. A computer readable medium storing program code for causing an issuing apparatus in a data storing system to perform processes, the data storing system comprising: a user apparatus which stores data; the issuing apparatus which is held by an issuer that provides the user apparatus, and issues and manages a registration certificate; a data providing apparatus which is held by a data provider that provides data; an issuer registration apparatus which is held by an issuer registrar that registers and manages the issuer; and a data registration apparatus which is held by a data registrar that registers and manages the data provider, the computer readable medium comprising:

program code means which receives user information and registration information on a key including a user public key or a part of a secret key from the user apparatus; and

registration generation program code means which generates registration certificate from the registration information and the user information, and sends the registration certificate to the user apparatus.

35

certificate and the storing data information for generating a storing authorization request when the registration certificate and the storing data information are verified; and

5 program code means which sends the registration certificate, the storing data information and the storing authorization request to the data providing apparatus;

 program code means which verifies a
10 storing authorization which is received from the data providing apparatus; and

 program code means which sends the storing authorization to the user apparatus when the storing authorization is verified.

15

39. The computer readable medium as
20 claimed in claim 36, further comprising:

 program code means which receives the registration certificate, storing data information and a storing authorization request from the data providing apparatus;

25 program code means which verifies the storing authorization request;

 program code means which provides certificate information to the storing authorization request and the storing data information when the
30 storing authorization request is verified for generating a storing authorization, and sends the storing authorization to the data providing apparatus.

35

00650323.082900

program code means which sends information
used for providing certificate information to the
5 issuer registration apparatus;

```

        program code means which stores the issuer
10  registration certificate when the issuer
    registration certificate is verified;

```

15 apparatus with the issuer registration certificate.

registration information generation means
35 which generates registration information on a key
including a user public key or a part of a secret
key, sends the registration information to the

issuing apparatus with user information; and
registration verification means which
verifies a registration certificate, received from
the issuing apparatus, which is signature
5 information or a hash value of the issuer for the
registration information and the user information,
stores the registration certificate to a storage
device when the registration certificate is
verified;
10 wherein the issuing apparatus comprises
registration generation means which generates the
registration certificate and sends the registration
certificate to the user apparatus,
the computer readable medium comprising:
15 program code means which receives the
certificate registration, storing data information
and a storing authorization request from the issuing
apparatus;
program code means which verifies the
20 storing authorization request;
program code means which provides
certificate information to the storing authorization
request and the storing data information when the
storing authorization request is verified for
25 generating a storing authorization, and sends the
storing authorization to the issuing apparatus.

30

42. The computer readable medium as
claimed in claim 41, further comprising:
program code means which verifies the
registration certificate and storing data
35 information which are received from the user
apparatus;
program code means which provides

00650323.002000

certificate information to the registration
certificate and the storing data information for
generating a storing authorization request when the
registration certificate and the storing data

5 information are verified; and

program code means which sends the
registration certificate, the storing data
information and the storing authorization request to
the issuing apparatus;

10 program code means which verifies a
storing authorization which is received from the
issuing apparatus; and

program code means which sends the storing
authorization to the user apparatus when the storing
15 authorization is verified.

20 43. The computer readable medium as
claimed in claim 41, further comprising:

program code means which receives the
registration certificate and storing data
information from the user apparatus;

25 program code means which verifies the
registration certificate;

program code means which generates a
storing authorization wherein certificate
information is provided to the registration
30 certificate and the storing data information when
the registration certificate is verified, and sends
the storing authorization to the user apparatus.

35

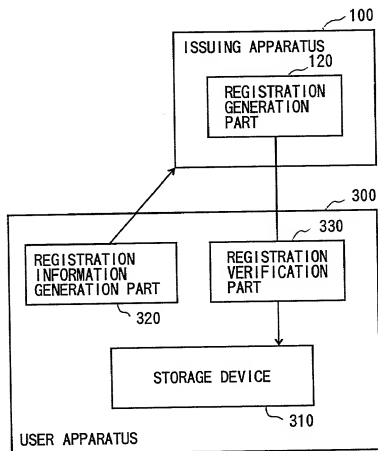
44. The computer readable medium as

00650323 "082000

A data storing system is provided, wherein the data storing system includes: a user apparatus; an issuing apparatus which issues a registration certificate; a data providing apparatus; an issuer registration apparatus; and a data registration apparatus; wherein the user apparatus includes: a part which generates registration information on a key including a user public key, sends the registration information to the issuing apparatus with user information; and a part which verifies a registration certificate, received from the issuing apparatus, which is signature information of the issuer for the registration information and the user information, stores the registration certificate to a storage device when the registration certificate is verified; wherein the issuing apparatus includes a part which generates the registration certificate and sends the registration certificate to the user apparatus.

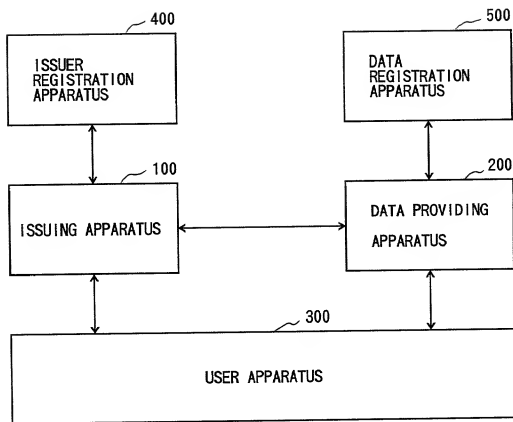
A data storing system is provided, wherein the data storing system includes: a user apparatus; an issuing apparatus which issues a registration certificate; a data providing apparatus; an issuer registration apparatus; and a data registration apparatus; wherein the user apparatus includes: a part which generates registration information on a key including a user public key, sends the registration information to the issuing apparatus with user information; and a part which verifies a registration certificate, received from the issuing apparatus, which is signature information of the issuer for the registration information and the user information, stores the registration certificate to a storage device when the registration certificate is verified; wherein the issuing apparatus includes a part which generates the registration certificate and sends the registration certificate to the user apparatus.

FIG. 1



006220-2205360

FIG. 2



000280 22305960

FIG. 3

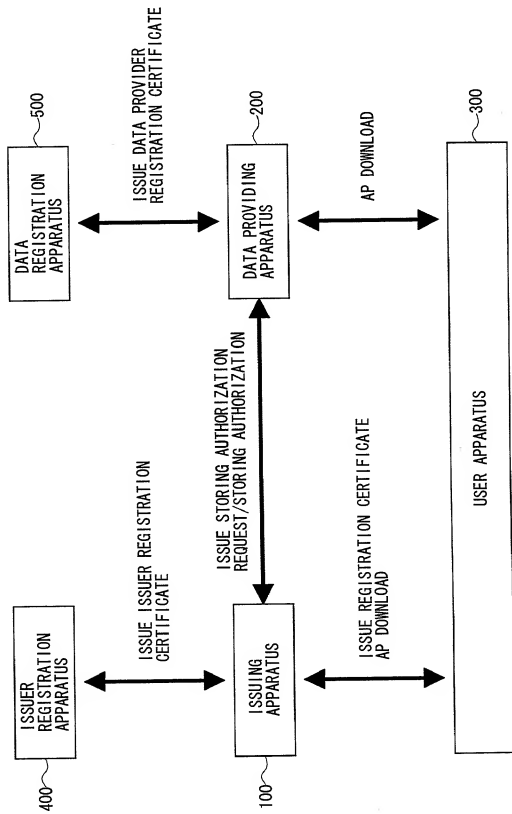


FIG. 4

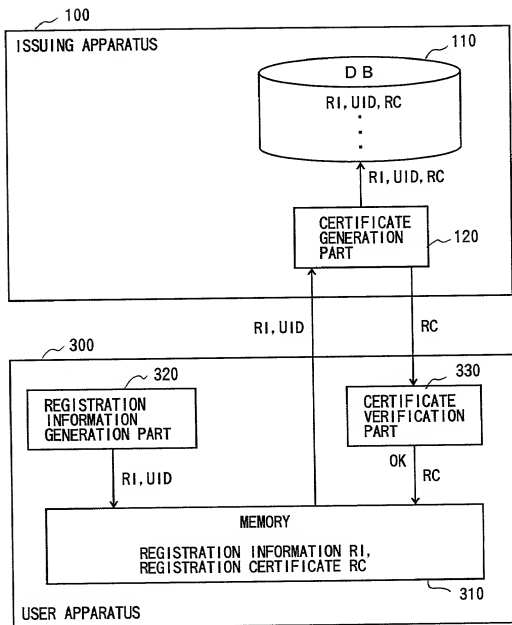


FIG. 5

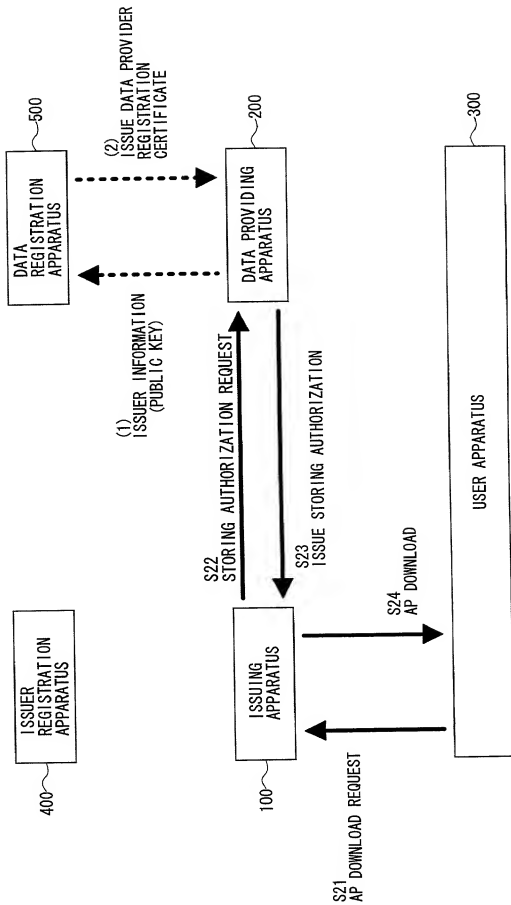


FIG. 6

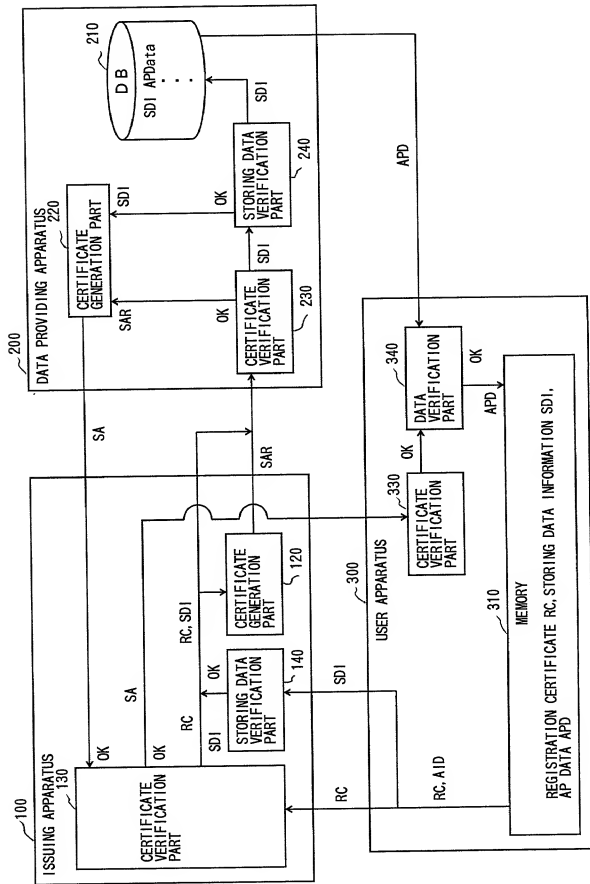


FIG. 7

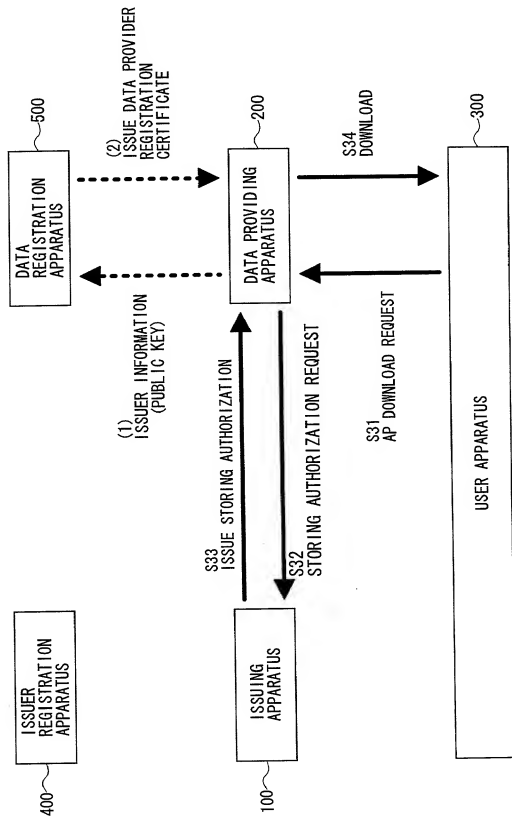


FIG. 8

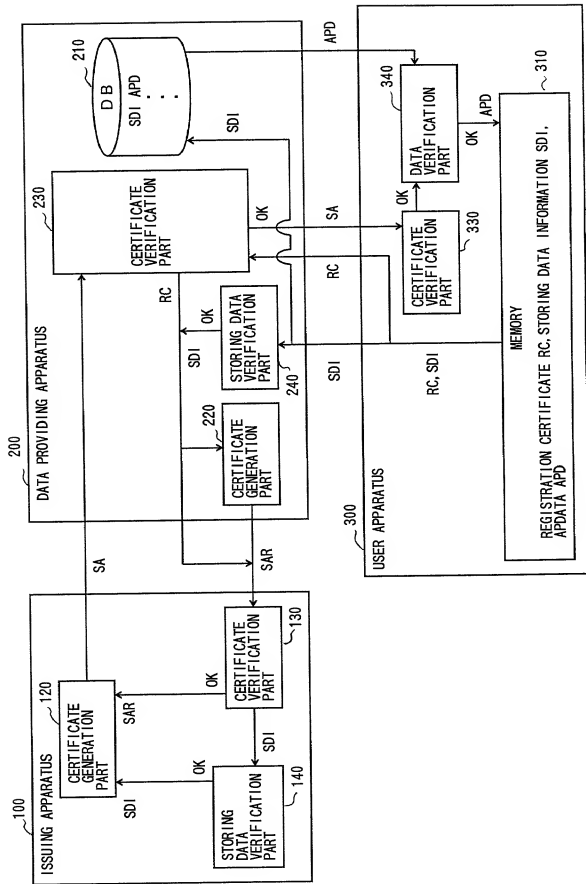


FIG. 9

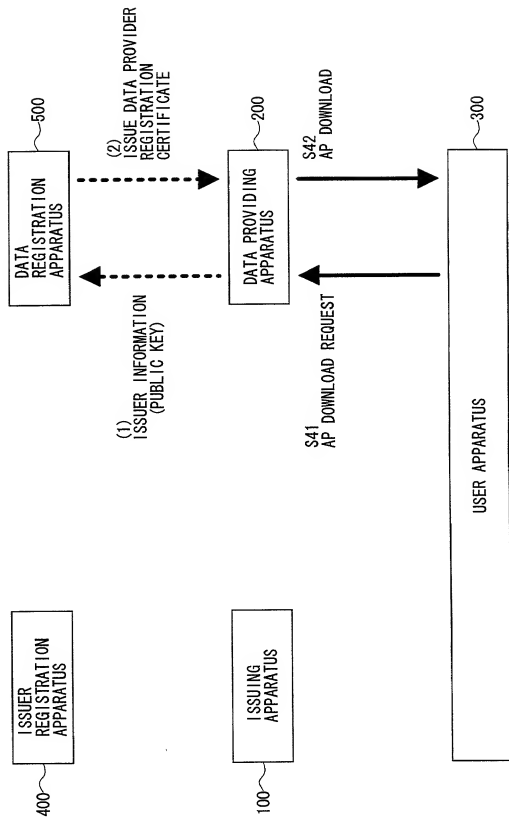
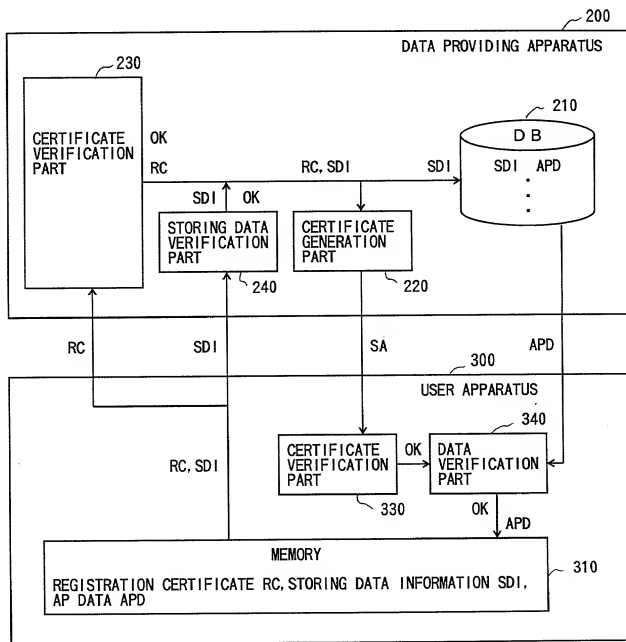


FIG. 10



006280-22505960

FIG. 11

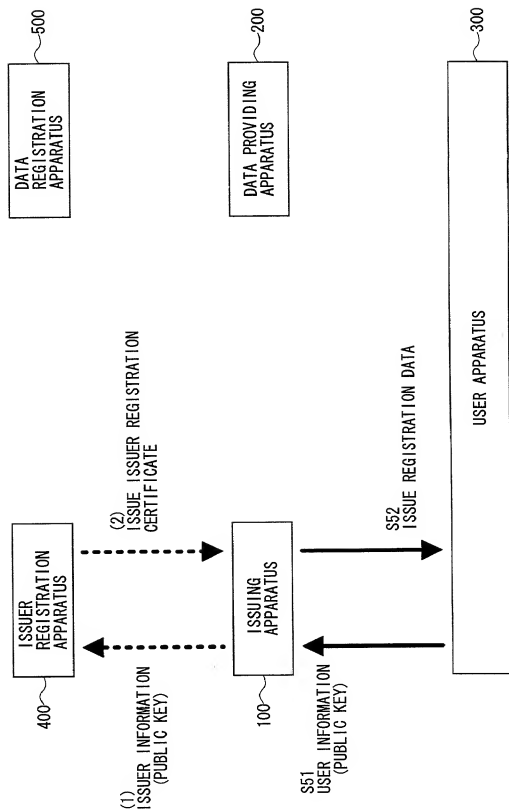


FIG. 12

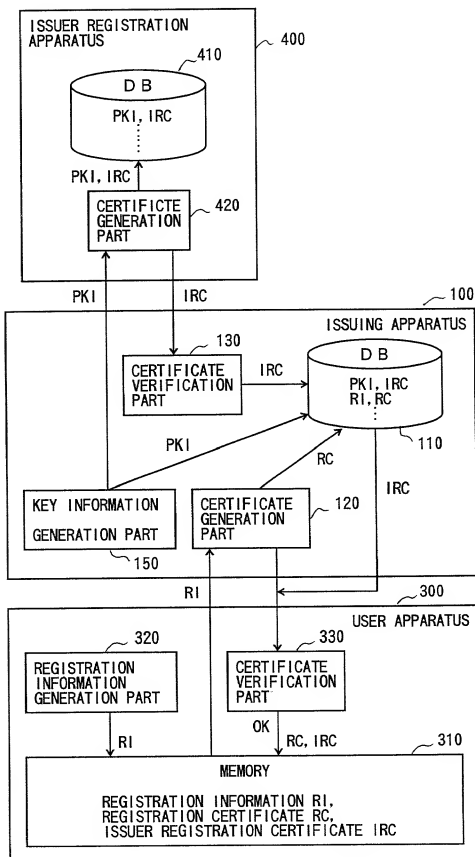


FIG. 13

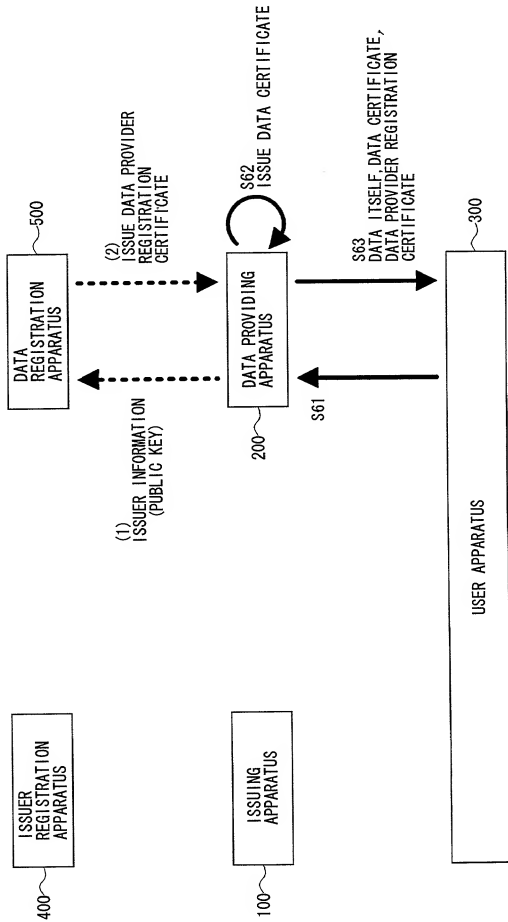


FIG. 14

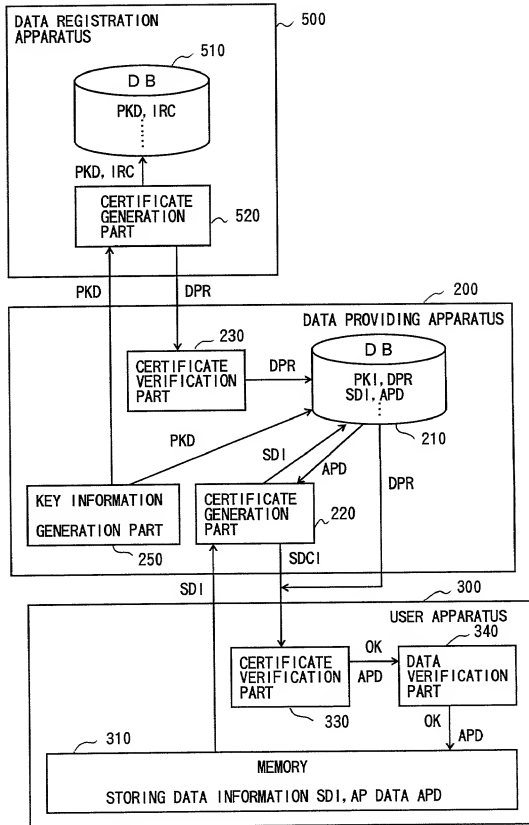


FIG. 15

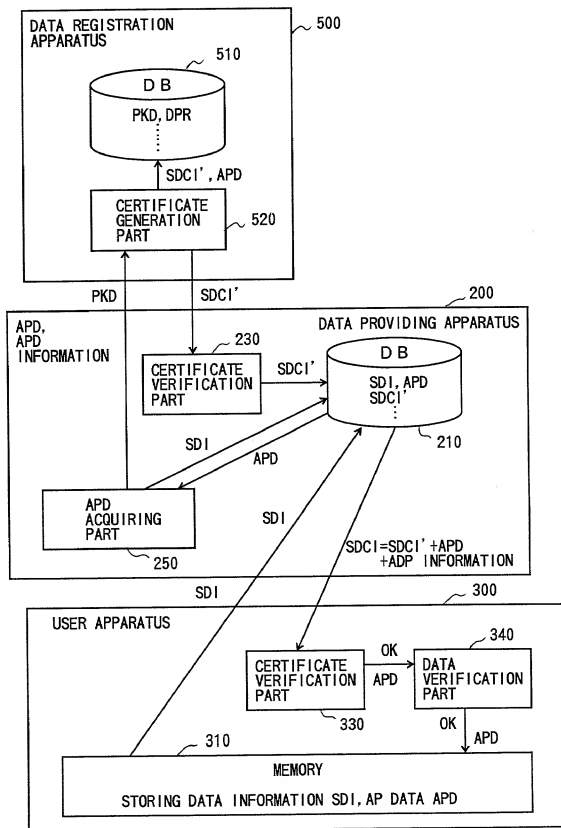
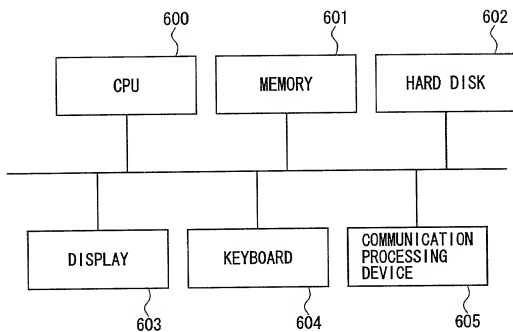


FIG. 16



006280-2235960

DECLARATION AND POWER OF ATTORNEY - ORIGINAL APPLICATION

ATTORNEY'S DOCKET NO.

As a below named inventor, I hereby declare that:
 My residence, post office address and citizenship are as stated below next to my name,
 I believe I am the original, first and sole inventor (if only one name is listed below) or
 an original, first and joint inventor (if plural names are listed below) of the subject matter which
 is claimed and for which a patent is sought on the invention entitled DATA STORING SYSTEM,
 ISSUING APPARATUS, DATA PROVIDING APPARATUS AND COMPUTER READABLE MEDIUM
 the specification of which STORING DATA STORING PROGRAM
 (check one)
☒ is attached hereto.
☐ was filed on _____ as Application Serial No. _____ and was
 amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified
 specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this
 application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any
 foreign application(s) for patent or inventor's certificate listed below and have also identified
 below any foreign application for patent or inventor's certificate having a filing date before that
 of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

COUNTRY	APPLICATION NUMBER	DATE OF FILING (day, month, year)	DATE OF ISSUE (day, month, year)	PRIORITY CLAIMED UNDER 35 USC 119
Japan	Pat. Appl. No. 11-243564	30/Aug./1999		<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
				<input type="checkbox"/> YES <input type="checkbox"/> NO

I hereby claim the benefit under Title 35, United States Code, §120 of any United States
 application(s) listed below and, insofar as the subject matter of each of the claims of this
 application is not disclosed in the prior United States application in the manner provided by the
 first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material
 information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the
 filing date of the prior application and the national or PCT international filing date of this
 application:

APPLICATION NO.	FILING DATE (day, month, year)	STATUS (i.e. Patented, Pending, Abandoned)

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this
 application and transact all business in the Patent and Trademark Office connected therewith. (List name and registration number)

Edward W. Greason, Esq.
 Reg. No. 18,918

SEND CORRESPONDENCE TO:

KENYON & KENYON
 One Broadway
 New York, New York 10004

DIRECT TELEPHONE CALLS TO:
(name and telephone number)

Edward W. Greason
 (212) 425-7200 X108

EL594605483US

00503231 002000

201	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECOND GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS as per attached	CITY as per attached	STATE & ZIP CODE/COUNTRY
202	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECOND GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS as per attached	CITY as per attached	STATE & ZIP CODE/COUNTRY
203	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECOND GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS as per attached	CITY as per attached	STATE & ZIP CODE/COUNTRY
204	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECOND GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS as per attached	CITY as per attached	STATE & ZIP CODE/COUNTRY
205	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECOND GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY
206	FULL NAME OF INVENTOR	FAMILY NAME	FIRST GIVEN NAME	SECOND GIVEN NAME
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP
	POST OFFICE ADDRESS	POST OFFICE ADDRESS	CITY	STATE & ZIP CODE/COUNTRY

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

SIGNATURE OF INVENTOR 201	SIGNATURE OF INVENTOR 202	SIGNATURE OF INVENTOR 203
Hideki Akashika	Shinichi Hirata	Nagaaki Ohya
DATE	DATE	DATE
August 22, 2000	August 22, 2000	August 22, 2000
SIGNATURE OF INVENTOR 204	SIGNATURE OF INVENTOR 205	SIGNATURE OF INVENTOR 206
Aki Kokubu		
DATE	DATE	DATE
August 22, 2000		

